

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.

THIS PAGE BLANK (USPTO)

暗号と情報セキュリティ

暗号と情報セキュリティ



辻井重男 編著
笠原正雄 著



暗号と情報セキュリティ
辻井重男 編著
笠原正雄 著

昭晃堂
総代理

定価(本体4,200円+税)

ISBN4-7856-3075-2 C3055 ¥4,200E

$$C = MC' + n \quad (5.76)$$

で与えられる。ここに n は MC' をさらに隠蔽するために付加するベクトルであり、重み $i \leq t$ の n 次元ベクトルである。

受信側においては、まず、

$$CP^{-1} = MSG + nP^{-1}$$

を得る。 P は置換行列であるから nP^{-1} は依然として重み i のベクトルである。したがって Goppa 符号の復号法を用いて nP^{-1} を訂正することにより MS を得ることができる。これより、

$$MSS^{-1} = M$$

として平文 M を復号することができる。この McEliece の公解鍵暗号では行列 S, P の選択に大きな自由度があるはか、Goppa 多項式 $G(Z)$ の選択にもかなりの自由度が存在する。このため McEliece 暗号は暗号として安全なものになると考えられている。

参考文献

- (1) W. W. Peterson and E. J. Weldon: "Error-correcting codes", Second Ed., MIT Press, 1972.
- (2) 笠原, 田崎, 小倉: "情報理論—基礎と応用—", 昭晃堂, 1985.

6. 認証とデジタル署名

高度情報化社会の出現とともに、通信技術とコンピュータ技術にささえられた情報システムを介して、情報交換が頻繁に行われるようになった。その結果、人間が対面することにより声や姿などから付随的に得られていた個人特有の情報 that 得られなくなり、情報交換に際して納得して行動することに支障が生じるようになった。情報システムを介して情報交換をしている相手は一体誰なのか、自分が発言した情報はまがいなく伝えられているか、また、何者かによって故意に改変されていないか、さらには、自分が特定の相手に伝えたものの情報は、本当に当人に伝えられたか、などをなんらかの手段により確認する必要がある。このような確認の機能を一般に認証 (authentication) という。また認証の機能をなんらかのアルゴリズムにより、機械的に実現するシステムを認証システムとよび、その実現手法としては暗号的手法 (cryptographic scheme) が有効である。したがって本章では暗号的手法を用いた認証とデジタル署名について解説しよう。

6.1 暗号と認証

暗号の機能は大きく分けて、情報の秘匿 (privacy) と認証 (authentication) に分類される。情報の秘匿とはなんらかの手段により情報が露呈されることがあっても、鍵がない限りその情報の意味がわからないようにして、第三者に対して情報の機密を守ることである。一方、契約や送金などが伴うビジネスの世界では、署名は欠かせない。電子郵便 (electronic mail) や電子送金 (electronic funds transfer) といった新しい形態のデータ通信では、文書の署名・捺印に相

当する、情報および送受信者の認証機能を備えていることが、ビジネスの上での争いを避けるためには必要不可欠である。

図 6.1 は暗号の機能を概念的に示したものである。一般に認証と呼ばれている機能は、

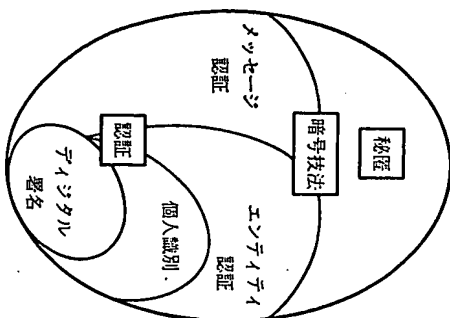


図 6.1 暗号技法の分類

- ① メッセージ認証 (message authentication)
- ② エンタイティ認証 (entity authentication)
および、これら両者の機能を兼ね備えた
- ③ デジタル署名 (digital signature)

に分けられる。

メッセージ認証とは、情報が改変されておらず、原情報のままの正しいものであることを保証する機能である。一方エンタイティ認証は、情報システムにおいて情報の生成・伝送・処理・記憶・判断などの行為に関与した実体 (エンタイティ) Aが、まさにそのエンタイティ A であることを保証する機能である。すなわち、エンタイティ A とエンタイティ B が協調するという条件の下に、A が B に A であることを証明できるが、第三のエンタイティ C が A になり

すまして、A であることを証明できないことを保証する機能である。

このようなエンタイティ A 認証において“当事者であるエンタイティ B 自身も第三のエンタイティ C に対して、A であることを証明できない”という条件を付加するとき、個人識別 (identification) というエンタイティ A 認証の機能になる。

デジタル署名には、メッセージ認証の機能とエンタイティ認証の機能という 2 面性のあることは、前述の通りである。これをエンタイティ A 認証の見地から見ると、個人識別の機能に“エンタイティ B が B 自身に対して A であることを証明できない”という条件をさらに付加することにより生まれる新しい機能が、デジタル署名ということになる。

個人識別とデジタル署名の概念の差異は微妙である。A と B の間でなんらかのトラブルが発生した場合に、B が問題となっているメッセージの送り主が確かに A であることを証明できる機能が個人識別である。さらにその事実を示す証拠を呈示することができ、かつ B が“にせ”のメッセージを偽造して、“そのメッセージの送り主が A である”と主張することができないとき、そのような機能をデジタル署名という。

図 6.2 はこのような階層構造をもつ 3 つのエンタイティ A 認証の機能を示している。

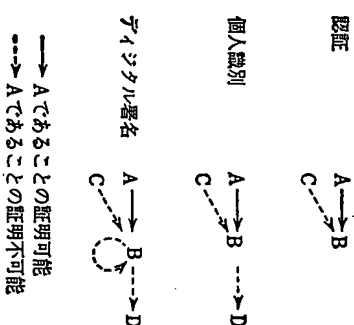
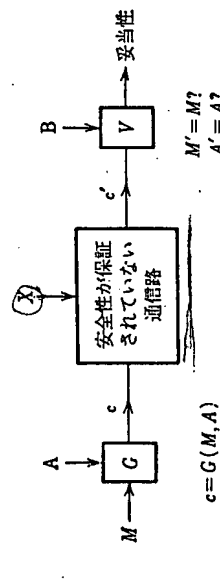


図 6.2 エンタイティ A 認証の階層構造

6.2 認証方式

認証方式の一般概念を図 6.3 に示す。図中 G はメッセージ M を通信文 c に



A, B: 合法的エンティティ G: 暗号アルゴリズム
X: 非合法的エンティティ V: 認証アルゴリズム

図 6.3 認証方式の一般的概念

変換するアルゴリズムであり、 V は受信した通信文 c' を認証するアルゴリズムである。A および B は情報システムに合法的に関与するエンティティを示し、 X は通信路に介在してメッセージを盗聴したり改ざんしたりする非合法的エンティティ (eavesdropper) を示す。まず A は通信文を生成アルゴリズム G を用いて、メッセージ M から c を生成し、必ずしも安全性が保証されていない通信路 (insecure channel) を通じて B に伝送する。通信路出力は一般に c' となる。通信文 c' を受信した B は認証アルゴリズム V を用いて、復元したメッセージ M' と A が送信したメッセージ M が等しいかどうか、ならびに受信側のエンティティ B が想定している相手が確かに A であるかどうかを検査し、その結果得られる妥当性 (validity) を出力する。これが認証方式の一般概念である。

このような一般概念から、図 6.4 に示すような認証方式を実現する 2 つの基本形が考えられる。図 6.4 の (a) は一体型、(b) は分離型と呼ばれている。まず図 6.4(a) の一体型では、2 つの変換アルゴリズム Γ およびその逆変換 Γ^{-1} が、それぞれ鍵 K_F および $K_{F^{-1}}$ により制御される暗号化・復号アルゴリズムを形成している。その出力のメッセージ M' が意味のあるものであれば、相手のエンティティ A およびメッセージが正しいことを認証できる。したがって

6.2 認証方式

認証と同時に秘匿の機能も兼ね備える認証のシステムが構成できる。このような認証方式は通信文復元法と呼ばれている。

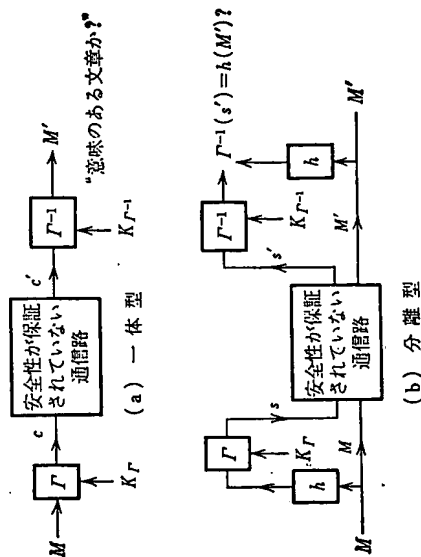


図 6.4 認証方式の基本形

図 6.4(b) の分離型は、メッセージ M を圧縮するなんらかのアルゴリズムが用いられることが特徴であり、普通縮約型のハッシュ関数 (hash function) h が用いられる。 Γ および Γ^{-1} は一体型と同様、鍵 K_F および $K_{F^{-1}}$ によって制御される 2 つの変換アルゴリズムである。また s は認証子 (authenticator) とよばれ、受信された認証子 s' に復号アルゴリズム Γ^{-1} を適用して得られる値 $\Gamma^{-1}(s')$ と受信されたメッセージ M' にハッシュ関数を用いて得られる値 $h(M')$ が一致するか否かによって、メッセージならびに相手のエンティティを認証できる。このような認証方式は認証子照合法と呼ばれている。

具体的な実現法としては、鍵 K_F および $K_{F^{-1}}$ により制御される変換 Γ および Γ^{-1} に、共通鍵暗号系 (common-key cryptosystem) の標準暗号としてよく知られている DES 暗号、FEAL 暗号などの暗号化・復号アルゴリズムを適用したり、RSA 暗号をはじめとする公開鍵暗号系 (public-key cryptosystem) の復号アルゴリズムおよび暗号化アルゴリズムを適用する方法が考えられる。ただし共通鍵暗号系を適用する場合には、 $K_F = K_{F^{-1}} = K$ (秘密) であり、公開、

鍵暗号系を適用する場合には $K_F = K_D$ (秘密), $K_F^{-1} = K_E$ (公開) かつ $E_{K_E}(D_{K_D}(M)) = M$ が成立しなければならない。

共通鍵暗号系を認証方式の基本形 (a) の一体型に適用するとき、実現できる認証システムは、最も制約条件のゆるやかなエンテライタ認証とメッセージ認証が同時に実現できる。しかしすべてのメッセージに暗号化および復号処理を施さなければならない。(b) の分離型の場合には、メッセージの秘匿の機能は失われるが、縮約型のハッシュ関数を用いてメッセージ M を圧縮して s ので、暗号化および復号処理を施すべきデータ量は少なくなる。

公開鍵暗号系を適用した認証システムは、暗号化鍵が公開されているので、後述するようにメッセージの秘匿機能のない認証システムとして位置づけることができる。しかし、暗号化・復号過程を~~と~~段~~わ~~けて少し工夫をこらすと、次に述べる最も制約条件の厳しいデジタル署名が実現できる。

6.3 デジタル署名

6.3.1 公開鍵暗号系を適用したデジタル署名

公開鍵暗号系⁽¹⁾を認証方式の基本形に適用すると、最も制約条件の厳しいエンテライタ認証であるデジタル署名が実現できる。ただし公開鍵 K_E が公開されているので、一体型の認証方式に適用する場合には、~~メッセージの~~秘匿の機能を備えることができない。すなわち、秘密鍵 K_D を用いてメッセージに暗号化処理を施して伝送しても、その暗号文を盗聴して公開の暗号化鍵 K_E により容易に平文のメッセージ M を得ることができる。前述の通り、一体型の認証システムではすべてのメッセージ M に暗号化処理を施すのであるから、もし可能ならば秘匿の機能も兼ね備えたいという要望が発生する。このような要望的確に答えたデジタル署名方式が存在するので、以下では秘匿の機能を有するデジタル署名方式について述べよう。

公開鍵暗号系の中には暗号化 E と復号 D の順序を交換できる暗号系、すなわち、

$$E_{K_E}[D_{K_D}(M)] = M \quad (6.1)$$

が支障なく実行できる公開鍵暗号系が存在する。RSA 暗号系⁽²⁾はその典型的な例である。式 (6.1) がなんら支障なく実行できるという前提条件の下に、一体型の認証方式を變形して、デジタル署名と同時に秘匿の機能も備わった認証システムを構成できる。図 6.5 はエンテライタ A からエンテライタ B へ秘密通信を行う場合を想定して構成した秘匿機能を備えた認証システムを示す。こ

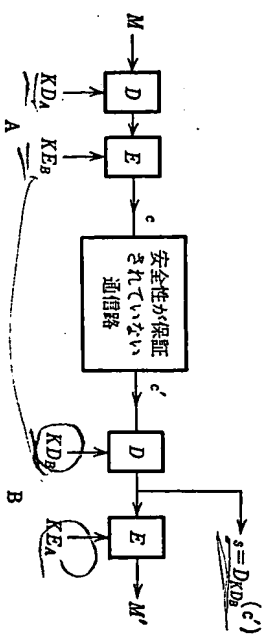


図 6.5 公開鍵暗号系を適用した認証システム

の認証システムの優れている点は、受信側で秘密鍵 K_{Da} を用いて c を復号した結果得られる値

$$s = D_{K_{Da}}[c] \quad (6.2)$$

を取り出せることである。すなわちエンテライタ A の公開鍵 K_{Ea} で s を暗号化することによりメッセージ M' が得られるので、もし M' が意味のある平文であれば、そのメッセージ $M' = M$ はエンテライタ A により送付されたものと断定できる。しかも受信者を含め A 以外のいかなるエンテライタもこの s を偽造できないので、B は s を保持することにより A が後でメッセージ M を送付した事実を否定できず、制約条件の最も厳しいデジタル署名方式になっている。

公開鍵暗号系を応用したデジタル署名方式を具体的に実現する際には、いろいろな解決すべき問題点が残されている。典型的な公開鍵暗号系としてよく知られている RSA 暗号系を用いて実現した場合にも次のような問題がある。

まず RSA 暗号系は次のように要約される (詳細は、第 3 章を参照されたい)。2 つの大きな素数 p, q をランダムに選び、それらの積 $n = pq$ を求める。 n は公開されるが、2 つの素数 p, q は秘密に保たれる。次に p, q を用いて n のオイ

ラー関数を,

$$\phi(n) = (p-1)(q-1) \quad (6.3)$$

により計算する。さらに秘密の $\phi(n)$ により規定される2つの条件

$$\begin{cases} \gcd(d, \phi(n)) = 1 \\ \max\{p, q\} < d < \phi(n) \end{cases} \quad (6.4)$$

$$(6.5)$$

を満たす整数 d を任意に選び合同式

$$ed \equiv 1 \pmod{\phi(n)} \quad (6.6)$$

を解いて e を求める。 e は公開鍵として公開リストに登録し、 d は秘密鍵として保持する。このような準備の下にエンティティAがエンティティBに秘密にメッセージを送送する場合、メッセージの1つのブロックを $M (0 \leq M \leq n-1)$ で表現し、公開鍵リストからBの公開鍵 $K_{D_B} = (e, n)$ を読み取り、暗号文

$$c \equiv M^e \pmod{n} \quad (6.7)$$

を計算してBに伝送する。この暗号文 c を受信したBは、秘密鍵 $K_{D_B} = (d, n)$ を用いて,

$$c^d \equiv M^{ed} \equiv M^{10(n)+1} \equiv M \pmod{n} \quad (6.8)$$

と計算し、メッセージ M を復元する。

このRSA暗号系を図6.5に示す認証システムに適用する場合、エンティティAとエンティティBの使用する n_A および n_B の値が異なるために、 $\text{mod } n_A$ と $\text{mod } n_B$ の計算の順序の違いにより計算結果が異なるという重要な問題が発生し、具体的な暗号化、復号並びに認証の方法を工夫しなければならない。このような問題に対し、Konfelderが明快な解決法を与えているのでその方法を紹介しておこう。

Konfelder⁽³⁾の暗号化および復号の方法は、 n_A と n_B の大小関係により二つの場合に分けて表6.1のように実行する。

このような暗号通信において、エンティティAとエンティティBの間でなんらかの争いが生じた場合には、調停者の助けを借りて表6.2のような方法で認証することにより解決できる。

表 6.1

	$\langle n_A < n_B \rangle$	$\langle n_A > n_B \rangle$
暗号化 復号	$c = E_{K_{E_A}} [D_{K_{D_A}}(M)]$ $M = E_{K_{E_A}} [D_{K_{D_B}}(c)]$	$c' = D_{K_{D_A}} [E_{K_{E_B}}(M)]$ $M = D_{K_{D_B}} [E_{K_{E_A}}(c')]$

表 6.2

	$\langle n_A < n_B \rangle$	$\langle n_A > n_B \rangle$
エンティティBが調停者に呈示	$M, x = D_{K_{D_B}}(c)$	M, c'
調停者の計算	$M' = E_{K_{E_A}}(x)$	$\begin{bmatrix} x = E_{K_{E_B}}(M), \\ x' = E_{K_{E_A}}(c') \end{bmatrix}$
判定条件	$M = M'$	$x = x'$

このようなKonfelderの方法では、modulusの大きい方を先に計算し、小さいmodulusによる計算を後で実行するように工夫されている点に着目すると容易に納得できる。またメッセージ M は、 n_A と n_B の小さい方よりも小さくなければならぬ。

6.3.2 離散対数問題に基づくデジタル署名

ElGamal公開鍵暗号系⁽⁴⁾の提案者として有名なElGamalは、同じ論文の中でElGamal暗号の考え方を応用したデジタル署名方式についても提案している。これは、大きな素数 P を法とする離散対数計算の困難さに基づくデジタル署名方式である。

ElGamalのデジタル署名方式の中心的役割を果たす離散対数問題 (discrete logarithm problem) は、次に示すような問題であり、一見簡単そうに見えるが実は極めて困難な問題なのである。いま大きな素数を P とし、 P を法として生成される有限体 $\text{GF}(P)$ の原始元を α とするとき、方程式

$$y \equiv \alpha^x \pmod{P} \quad (6.9)$$

において、 x より y を求めることは容易であるが、 y が与えられたとき x を求めることは、極めて困難な問題である。このような一方向性関数を用いて、次のようなデジタル署名方式が実現できる。

エンティティAが署名し、エンティティBが認証する場合を考えよう。まず

準備として、エンテイティAは大きな素数 P を選び、これを公開する。また乱数 $x_A (0 \leq x_A < P-1)$ を生成し、これをAの秘密鍵とする。さらに x_A と α を用いて、

$$y_A \equiv \alpha^{x_A} \pmod{P} \quad (6.10)$$

を計算し、 α と y_A を公開する。ここで y_A を公開しても秘密鍵 x_A が割り出せないのは、離散対数問題の困難さに基づいている。

いま署名を行うメッセージを $M (0 \leq M < P-1)$ とすると、次式を満足する r と s の対 (r, s) を M の署名とする。

$$\alpha^M \equiv g^{r \cdot r' + s \cdot s'} \pmod{P} \quad (6.11)$$

エンテイティAは固有の秘密鍵 x_A を保持しているのて、次のようにして署名 (r, s) を作成できる。

$$(i) \quad \gcd(k, P-1) = 1 \text{ および } 0 \leq k < P-1 \text{ を満たす乱数 } k \text{ を選ぶ。}$$

$$(ii) \quad k \text{ および } \alpha \text{ を用いて、} r \text{ を次式により計算する。}$$

$$r \equiv \alpha^k \pmod{P} \quad (6.12)$$

$$(iii) \quad \text{式 (6.12) を式 (6.11) に代入すると、}$$

$$\alpha^M \equiv \alpha^{x_A r' + k s'} \pmod{P} \quad (6.13)$$

となり、

$$M \equiv x_A r' + k s' \pmod{P-1} \quad (6.14)$$

が得られるので、 s について解くことにより、署名 (r, s) が得られる。なお s の一意性は、 k が(i)の条件を満たすことにより保証されている。

メッセージ M および署名 (r, s) を受信したエンテイティBは、式(6.11)が成立することを確認することにより、Aの署名の正当性を認証できる。

なお、同じ k を二度と使用しないように注意しなければならない。なぜならば、異なるメッセージの署名に同じ k の値を使用すると、式(6.14)より x_A および k を未知数とする連立方程式

$$M = x_A r + k s$$

$$M' = x_A r + k s'$$

が得られ、 x_A が算出できるからである。

6.3.3 ナツナザツク問題に基づくデジタル署名

MH法と呼ばれているナツナザツク問題に基づく公開鍵暗号系⁹⁾は、式(6.1)を支障なく実行できるという条件を満たすために、デジタル署名には適していない。しかしShamirはナツナザツク問題のNP完全性に着眼し、MH法を直接適用する方法とは異なった考え方でナツナザツク問題に基づくデジタル署名法を提案している¹⁰⁾。

まず簡単に署名の原理を説明しよう。 k ビットで表現される任意の素数を n 、整数表示したメッセージを $M (0 \leq M \leq n-1)$ 、1つの正整数ベクトルを $a = (a_1, a_2, \dots, a_{2k})$ とすると、 $M \equiv ca \pmod{n}$ 、すなわち、

$$M \equiv \prod_{j=1}^{2k} c_j a_j \pmod{n} \quad (6.15)$$

を満足する正整数ベクトル $c = (c_1, c_2, \dots, c_{2k})$ 、 $0 \leq c_j \leq [\log_2 n]$ を求めるナツナザツク問題は、NP完全である。ここでナツナザツク問題の解であるベクトル c を署名と考えると、署名の検証は、

$$ca \pmod{n} \equiv M \quad (6.16)$$

によりきわめて容易に実現できる。また署名を偽造するためには、式(6.15)で与えられるNP完全なナツナザツク問題を解く必要があり、異なるメッセージ M' に署名することは、きわめて困難である。

しかし上述の署名の原理によれば、正当な署名者にとっても c を計算することとは、きわめて困難である。そこでトラツナブアとして大きな役割を果たす秘密の情報を k 行 $2k$ 列の乱数行列 $H = [H_{ij}]$ により与え、

$$\begin{bmatrix} h_{1,1} & h_{1,2} & \dots & h_{1,2k} \\ h_{2,1} & h_{2,2} & \dots & h_{2,2k} \\ \dots & \dots & \dots & \dots \\ h_{k,1} & h_{k,2} & \dots & h_{k,2k} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \dots \\ a_{2k} \end{bmatrix} \equiv \begin{bmatrix} 2^0 \\ 2^1 \\ \dots \\ 2^{k-1} \end{bmatrix} \pmod{n} \quad (6.17)$$

を満足するベクトル $a = (a_1, a_2, \dots, a_{2k})$ を計算し公開する。上式(6.17)は $2k$

個の未知数を含む k 個の方程式であるから、 a_1 から a_k まではランダムに選ぶことができる。 a_{k+1} から a_n までは k 個の線形方程式を連立して解くことにより求められる。

いまメッセージを M ($0 \leq M \leq n-1$) とし、 M の 2 進表現の各ビットを、左側を下位として並べたベクトルを m で示すと、メッセージ M に対する署名は次式により決定できる。

$$c = mH \quad (6.18)$$

また署名 c の検証は c と a を用いて、

$$\begin{aligned} ca \bmod n &\equiv \sum_{j=1}^n c_j a_j \bmod n \equiv \sum_{j=1}^n \left[\sum_{i=1}^n m_i h_{ij} \right] a_j \bmod n \\ &\equiv \sum_{i=1}^n m_i \left[\sum_{j=1}^n h_{ij} a_j \right] \bmod n \equiv \sum_{i=1}^n m_i 2^{i-1} \bmod n \equiv M \end{aligned} \quad (6.19)$$

となるので、送信された M との一致性を確認すればよい。

上述の署名法は完全な方式のように思われるが、数多くの M と c の対を集めると上式 (6.18) より H を決定できる。これを防止するためには、署名する前にメッセージをランダム化すればよい。まずランダムな 2 進ベクトルを $r = (r_1, r_2, \dots, r_n)$ とし、

$$M^* \equiv (M - ra) \bmod n \quad (6.20)$$

を計算する。その結果 M は M^* を用いて、

$$M \equiv (M^* + ra) \bmod n \quad (6.21)$$

と記述できる。つきに上述の署名方式を適用して M^* を署名し c^* を得る。この c^* に r を加えて得られる値

$$c = c^* + r \quad (6.22)$$

を署名とする。

署名 c の検証は次式のようにして容易に実行できる。

$$\begin{aligned} ca \bmod n &\equiv (c^* + r)a \bmod n \\ &\equiv c^*a + ra \bmod n \\ &\equiv (M^* + ra) \bmod n \end{aligned}$$

$$\equiv M \quad (6.23)$$

このように修正すれば、数多くの M と c の対を集めても、行列 H の要素を算出することはきわめて困難になる。

6.4 ID 情報に基づくデジタル署名

固有の情報 (identity information, ID) に基づく暗号系と署名法の基本概念は、1984 年に開催された CRYPTO' 84 において Shamir⁽⁷⁾ により提案された大変興味深いユニークな発想である。この節では、まず ID 情報に基づく暗号系と署名法の基本概念を示し、次に Shamir 自身により提案されたデジタル署名法について紹介しよう。

6.4.1 ID に基づく暗号系と署名法の基本概念

送受信者間で公開鍵や秘密鍵を交換する必要が全くなく、また鍵のリストや第三者によるサービスも必要としない方法で、任意のエンティティ間で安全に通信ができ、かつ互いに署名を認証できる新しい暗号化方式である。この方法は信頼できる鍵生成センタの存在を仮定している。鍵生成センタを設置する唯一の目的は、新規にエンティティが情報ネットワークに加入する時に、そのエンティティの名前や住所、電話番号などの固有の情報を受け取り、センダ固有の秘密のアルゴリズムを用いて、その ID に対応する秘密鍵を生成し、個人ベースで使用するスマートカードに記録して発行することである。このカードの中に収められている秘密の情報により、通信相手が変わっても各エンティティは全く独自に自分の送るメッセージを暗号化したり署名を行うことができる。また自分の受け取る暗号文の復号や認証を行うことができる。ID に基づく暗号系と署名法の概念を図 6.6 および図 6.7 に示す。

ID に基づく暗号系と署名法は、公開鍵として ID を使用し、共通の秘密鍵生成アルゴリズムを鍵生成センタ固有の秘密情報とする、公開鍵暗号方式であると考えられる。